CHAPTER 6
COMPUTER SECURITY AND ETHICS

SHORT AND LONG QUESTIONS

Q.1 Define cybercrime.

Ans: Cybercrime:

Cybercrime refers to any crime that is committed by means of computer and Internet technology by having unlawful access to others' computers.

Many governments have passed cybercrime bill that carry fines and prison sentences for cybercriminals.

Q.2 Describe some commonly committed cybercrimes.

Ans: Commonly committed cybercrimes:

The following are the commonly committed cybercrimes.

i. Computers have been involved in crimes such as fraud, kidnapping, murder and crimes related with stealing money from bank and credit card company.

ii. Criminals use Internet to steal personal information of other users and commit various types of cybercrimes. Personal information includes username, password, credit card number, bank account number, etc.

iii. Downloading illegal software, music files and videos are also cybercrimes.

iv. Internet harassment or cyber bullying is also a serious crime committed by cybercriminals. Internet harassment includes sending threatening e-mail, spreading rumors or virus, making defamatory comments, sending pornography or other bad material.

v. Making negative comments about an individual on Internet can damage reputation or cause physical or mental harm to the victim.

Q.3 What are computer viruses?

Ans: Computer Viruses:

Some computer experts create malware such as virus, spyware, worm etc. and spread through Internet. It is very importance to understand how malware spreads and how to protect computer from them.

It is very difficult to list all the symptoms of infected computers. The reason for this is that there are hundreds and thousands of malicious programs and new ones are created every day. Sometime, some infected computers do not show any symptom and the user thinks that his computer is not infected.

For Your Information

Firewall is a software or piece of hardware used to prevent unauthorized Internet users from accessing computer systems that are connected to Internet.

Tip

To create a strong password, you should combine upper-case and lower-case letters, numbers and special symbols.

Q.4 Describe the term multimodal authentication.

Ans: Multimodal Authentication:

Multimodal authentication means combination of two or more types of authentication methods. Normally, authentication methods use a single source of information for authentication such as features of face, fingerprint, hand geometry, access cards, etc. Multimodal authentication uses multiple sources of information for identification.

For example, fingerprint and face recognition can be combined for a multimodal biometric authentication system. As another example, a multimodal authentication can combine access card and PIN to open security gate.

Q.5 Describe computer ethics in information accuracy, information ownership, intellectual property rights, software piracy and information privacy.

Ans: Areas of Computer Ethics:

The following are main areas of computer ethics.

- Information accuracy
- Information ownership/Intellectual rights
- Intellectual Property
- Software piracy
- Information privacy
- Internet and Privacy

Information Accuracy:

Information stored on computers must be accurate, up-to-date and complete. If wrong information is entered in computer, it can be very harmful. People may suffer because of inaccurate information stored on computer. For example, a credit card holder may be wrongly blacklisted if wrong information is entered into the computer.

Information Ownership/Intellectual Rights:

Information ownership or intellectual rights mean persons who create ideas in any form are the actual owners. Ideas may be in the form of poems, plays, novels, films, drawings, paintings, software, etc. Intellectual rights protect creative work from unauthorized use by other people and allow creators to benefit financially from their work.

Intellectual Property:

Intellectual property means the legal rights of an individual or a corporation that result from intellectual activity in literary, artistic, scientific and industrial fields. Countries have law to protect intellectual property to foster innovation and promote creativity.

Software Piracy:

Software piracy means making illegal copies of software for use or sale for financial benefit. When computer users buy licensed software, they have the right to use it on a single computer. Software Copyright Law does not allow to make illegal copies of software and install it on other computers or sell it. It allows software developers to benefit financially from their work.

Information Privacy:

Information privacy refers to an individual's right to the privacy of personal information. In modern information age, people are concerned that computers may be taking away their privacy. The Data Protection Act (Law) protects the rights of the individuals against misuse of personal information by organizations. Organizations that hold the information should not allow unauthorized people to have access to information or disclose it to anyone outside the organization.

Internet and Privacy:

People who use Internet are worried that it may be eroding their privacy. Internet users post their personal information such as full name, date of birth, place of residence, phone numbers, pictures, videos etc. on the Web and it stays there. Internet users enter personal information in websites to sign up or register for services without realizing that this may lead to invasions of privacy. This information can be accessed by hackers and used for harmful purpose. This poses a serious threat to privacy as unauthorized people can access personal information of individuals. Therefore, people are concerned about invasion of computer and Internet technology into people's privacy.

KEY POINTS

- Computer security refers to protecting computer hardware, software and information stored on computer from threats.
- A crime that is committed by means of computer and Internet technology is known is cybercrime.
- A person who illegally breaks into others' computer systems is known as hacker.
- A person who uses special tools for breaking into computer systems is known as cracker.
- Malware means malicious software. It comprises of harmful software such as virus, worm, spyware etc. that are threats to all computer users.
- Malware spreads through infected flash drives, CDs, pirated software, Internet, e-mail attachments and devices that are plugged into computer's USB ports.
- Authentication means identifying a person based on a method such as Username and Password, Personal Identification Number, Access Card or Biometrics.
- Authorization verifies that an authenticated person has permission to access computer system and use it.

- Personal Identification Number (PIN) is a confidential numeric password used to authenticate a user to get access to computer system.
- Access cards are very similar in appearance to credit cards. They are used to open security gates, parking barrier and doors of hotel rooms.
- Biometrics is a method based on measurement of features of face, fingerprint, hand geometry, signature and voice for authentication of individuals.
- Multimodal authentication combines two or more types of authentication methods such as face and fingerprint for identification of individuals.
- Computer ethics is concerned with the moral guidelines for the ethical use of computer technology. It specifies what is right and what is wrong when using computers.
- Information ownership or intellectual rights mean a person who creates an idea in any form is the actual owner. Intellectual rights protect creative work from unauthorized users and allows creator to benefit financially.
- Software piracy means making illegal copies of computer software for use or sale for financial benefit.

EXERCISE

Q1. Select the best answer for the following MCQs.

i. What is a person who illegally breaks into others' computer systems called?

A.	Computer engineer	B.	System programmer
C.	Hacker	D.	Cracker

ii. What is a person who uses special tools for breaking into computer systems called?

A.	Computer engineer	B.	System programmer
C.	Hacker	D.	Cracker

iii. Which malware spreads automatically in computer networks and replicates itself?

A.	Virus	B.	Worm
C.	Adware	D.	Spyware

iv. Which of the following malware displays advertisements on the screen?

A.	Virus	B.	Worm
C.	Adware	D.	Trojan

v. Which of the following authentication method is used for opening security gates?

A.	Username and password	B.	Personal Identification Number
C.	Access card	D.	Biometrics

vi. Which of the following authentication method is most reliable?

A.	Username and password	B.	Personal Identification Number
C.	Access card	D.	Biometrics

vii. **Which of the following authentication method is based on features of individuals such as face, fingerprint and voice?**

A. Username and password B. Personal Identification Number
C. Access card D. Biometrics

viii. **What is making illegal copies of copyright software for use on other computers or sale called?**

A. Information privacy B. Intellectual rights
C. Software piracy D. Information ownership

ix. **Which of the following malware gathers information about user activities on computer?**

A. Virus B. Worm
C. Adware D. Spyware

x. **Which of the following authentication methodology is used to draw cash from ATM?**

A. Username and password B. Personal Identification Number
C. Access card D. Biometrics

Answers

i. C	ii. D	iii. B	iv. C	v. C
vi. D	vii. D	viii. C	ix. D	x. B

Q2. Write short answers of the following questions.

i. Define cybercrime.

Ans: Cybercrime:

Cybercrime refers to any crime that is committed by means of computer and Internet technology by having unlawful access to others' computers.

ii. What is the importance of computer security?

Ans: Computer Security:

Computer security refers to protecting computer hardware, software and information stored on computer from threats.

Importance of Computer Security:

Computer users often exchange information with each other or communicate over Internet. This can infect a user's computer with virus or other types of malicious software.

Computer security or safety is important for computer users to protect their computer from different threats. It is necessary to install security software such as firewall, antivirus and spyware on computers.

iii. Differentiate between hacker and cracker.

Ans: Hacker:

A person who illegally breaks into others' computer systems is known as hacker. Hacking is a cybercrime.

- Hackers are computer experts who try to gain unauthorized access to computer systems for stealing and corrupting information.
- Most of the hackers break into computers for financial benefits. They try to get credit cart details or bank account information so that they can steal money.

- Hackers have in-depth knowledge of network programming and can create tools and malicious software for others to break into networks and create problems.

Example:

For example, a hacker develops software in which a dictionary file is loaded that contains all the dictionary words. When the software is run it tries all the dictionary words one by one as password to hack a computer. This method works if the user is having a simple password that exists in the dictionary.

Cracker:

Cracker is a computer user who breaks into computer systems without permission using hacking tools for personal gain or damage and commits cybercrimes.

- Most of the crackers do not have professional computer skill to hack computer systems but they have knowledge about using hacking tools.
- Crackers break into computers and cause serious damage. They also break into Web servers and replace the home page of a website with a page of their own design.
- These criminals are dangerous and harder to catch.

Example:

For example, a cracker can install a key logger on another user's computer through Internet. A key-logger is software which records every typed letter on the keyboard. When the user uses Facebook and enters the Facebook account details, it will get recorded in the cracker's computer. Now, he can easily hack the Facebook account.

iv. Describe any five symptoms of malware.

Ans: Common Symptoms of Malware Attacks:

A list of common symptoms of infected computers is given below.

- The computer does not start or it reboots automatically when it is on.
- Different types of error messages appear on the screen.
- Unexpected messages appear on the screen.
- Programs do not run in a normal way.
- Computer is running very slow.
- New files or folders are created on the hard disk.
- Folders are deleted or changed on the hard disk.
- Hard disk activity is noticed without running any program.
- Web browser does not run in a normal way.
- Strange noise is heard when the computer is on.

v. Differentiate between authentication and authorization.

Ans: Authentication:

Authentication means identifying a person based on a method such as Username and Password, Personal Identification Number (PIN), Access Card or Biometrics. It verifies who the person is.

Authorization:

Authorization means to give someone permission to do something.

Example:

For example when a user wants to login to his email account, he is asked to enter username and password to verify his identity. This is authentication.

If correct username and password are entered, the user is authorized or allowed to check his emails, send email or perform other tasks related with email service. This is authorization

vi. Which authentication methodology provides highly secure identification and verification? Justify your answer.

Ans: Biometrics provides highly secure identification and personal verification technologies.

Biometrics refers to authentication methods based on physical characteristics of individuals such as features of face, hand geometry, retina, voice and fingerprint.

Biometrics based systems are used for financial transactions, electronic banking and personal data privacy.

Biometrics provides more accurate authentication than using username and password or PIN. Biometrics is associated with a particular individual. Hence, it cannot be borrowed, stolen or forgotten. Forging in biometrics is practically impossible.

vii. What is meant by information privacy?

Ans: Information Privacy:

Information privacy refers to an individual's right to the privacy of personal information. In modern information age, people are concerned that computers may be taking away their privacy.

The Data Protection Act (Law) protects the rights of the individuals against misuse of personal information by organizations. Organizations that hold the information should not allow unauthorized people to have access to information or disclose it to anyone outside the organization.

viii. Give any three drawbacks of software piracy?

Ans: Disadvantages/Drawbacks of software piracy:

Pirated Software:

Software piracy refers to making of unauthorized copies of copyrighted software and distributing it. Pirated software on CDs is a very common source of spreading malware on computers because these are often infected.

If users download pirated music, movies, programs, etc. for free, their computers may be infected because pirated downloads often contain viruses, spyware or other malicious programs.

OR (Second Answer)

1. **It's illegal:** making unauthorized copies of software is a federal crime.
2. **It's risky:** if you downloading pirated software from internet, it is more likely to be infected with computer viruses which can damage your computer system.
3. They do not provide after-sales services.
4. Software piracy slows the economic growth rates of developing because it discourages new software developers from entering the market and slows down the industry's ability to bring new and innovative solutions to consumers.

5. Downloading files illegally have a risk of viruses and Spyware! Pirated software can carry viruses or may not function at all.
6. Unlicensed users do not receive quality documentation. It also deprives consumers of the basic protections offered by properly licensed software like money-back guarantees, installation support, maintenance releases, and upgrade rebates.
7. Piracy can expose end-users to potential risks of identity theft if criminals who sell counterfeit software CDs obtain a buyer's name, address, credit card and other information during purchase. This increases identity theft risks.

ix. What types of problems may be faced if computer users do not comply with the moral guidelines of computer ethics?

Ans:

1. Computer users can use Computer to harm other people.
2. Computer users can use Computer to break into others' computer systems to steal, change or destroy information.
3. Computer users can read documents and e-mails of other users without their consent.
4. Computer users can use Computer to make illegal copies of copyright software and sell it for financial benefit.
5. Computer users who have special computer knowledge and ability will create malicious software (such as computer virus) and spread it to other computers.
6. Computer users can commit any type of crime with the help of computer technology.
7. Computer users can not respect the privacy of others.

x. Name any three places where authentication of people is required.

Ans: Username and password are used to authorize users to have access to computer systems, e-mail account, bank account and other services available on computer.

PINS are most commonly used with debit and credit cards in retail stores and many other places for payment of bills. It is also used with ATM cards to withdraw cash from ATM machines.

Access cards are commonly used to open security gates in offices where unauthorized people are not allowed to enter. Access cards are also used to open barriers in parking areas. They are an alternative to key for opening hotel room, etc.

Biometrics provides highly secure identification and personal verification technologies. Biometrics based systems are used for financial transactions, electronic banking and personal data privacy.

Q3. Write long answers of the following questions.

i. Define malware and describe its types.

Ans: Malware:

Malware is malicious software. It comprises of a number of harmful software that are threats to all computer users. Malware is created for attack on privacy, spying, destruction and financial benefits.

Types of malware:

Most common types of malware are:

- Computer viruses
- Spyware
- Worms
- Adware

- **Computer Viruses:**

A computer virus is a type of malware that spreads by inserting a copy of itself into another program or file.

i. Most of the viruses are attached to executable files.

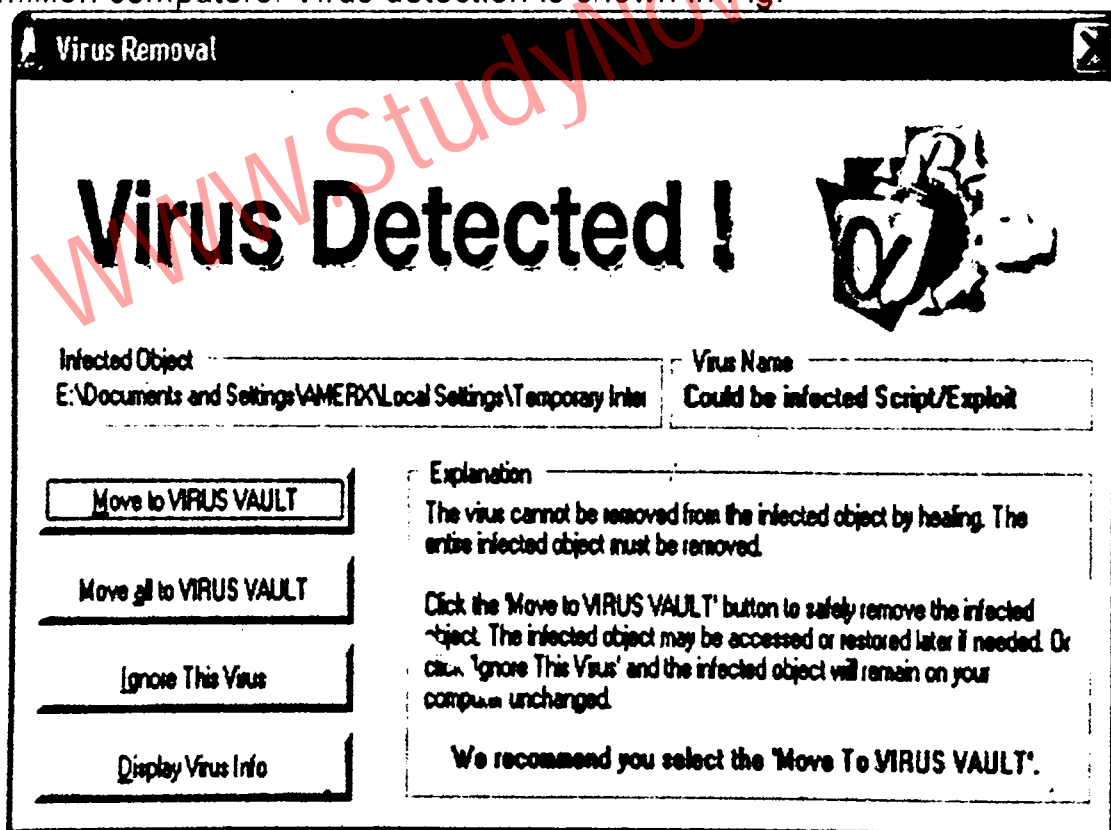
ii. Viruses spread and infect other files when a computer user opens the infected program or file.

iii. Viruses also spread when infected files are transferred from one computer to another through network, USB flash drive, CD/DVD or infected e-mail attachments.

iv. Some viruses are not very harmful they are simply annoying while others can seriously damage the hardware, software or the information stored on the computer.

v. Viruses can slow down the computer and some can even stop its operation.

Examples of viruses:

Examples of viruses are I Love You, MyDoom, etc. I Love You is an e-mail virus that infected computer when user opened an e-mail attachment named "I Love You" MyDoom virus was discovered in 2004. It quickly infected about one million computers. Virus detection is shown in Fig.

Detection of computer virus by antivirus software

Worms:

A worm is a malware that transmits itself over a network to infect other computers.

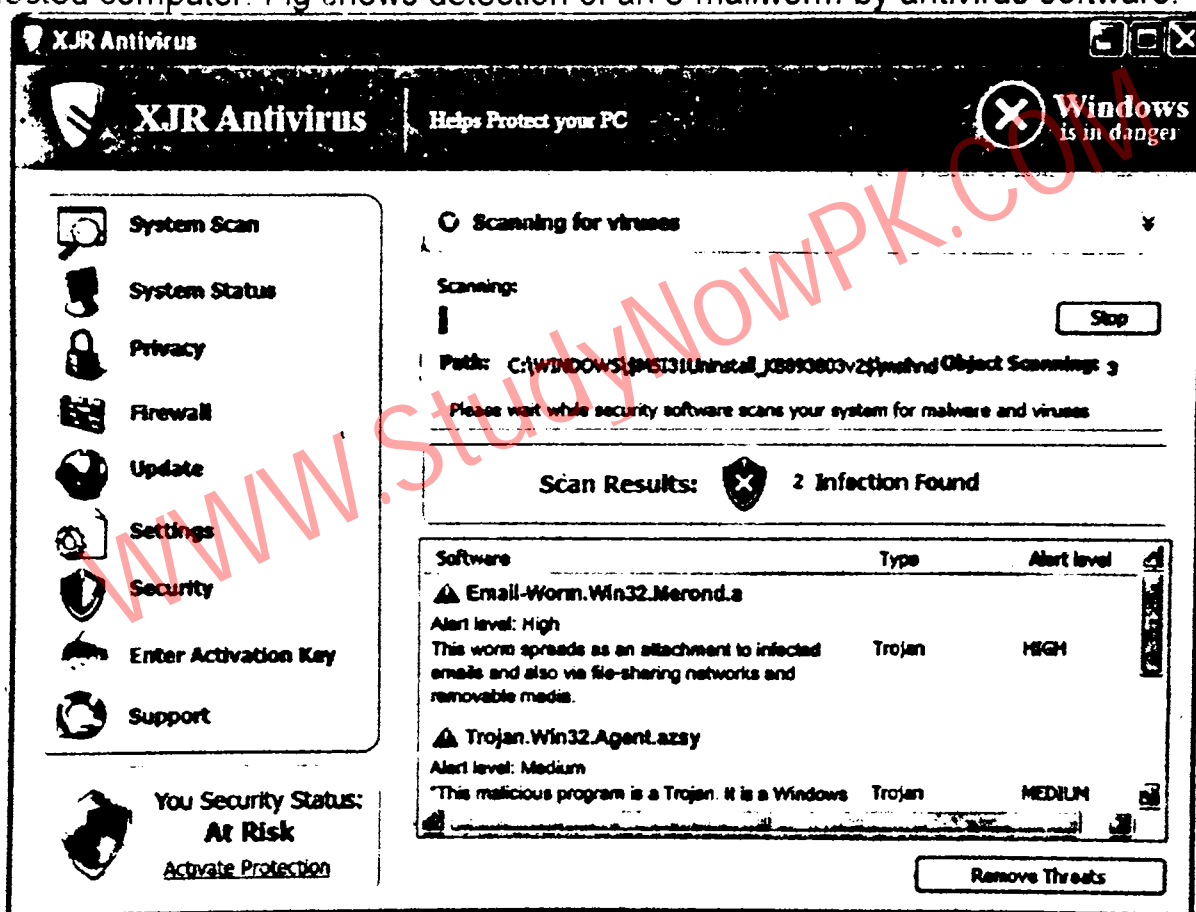
i. Worm can be harmful like a virus.

ii. It spreads automatically in computer networks and replicates itself. It can travel from computer to computer without any human action.

iii. It enters a computer through a weakness in the operating system of the computer.

iv. Most of the worms cause some harm to the network such as slowing down communication by increasing network traffic.

Examples of Worms:

Code Red and Fizzer are examples of worms. Code Red worm broke out in July, 2001 and infected about 360,000 computers in a single day. Fizzer is a mass-mailing worm that captures a user's keystrokes and can allow the attacker access to infected computer. Fig shows detection of an e-mailworm by antivirus software.

Detection of worm by anitvirus software

For Your Information

The first computer virus named 'Brain' was created by two Pakistani brothers, Basit Farooq Alvi and Amjad Farooq Alvi in Lahore in 1986.

Spyware:

Spyware programs are developed to spy on computer users by gathering information about their activities on the computer.

i. Spyware is developed for the personal benefit of the creator.
ii. It performs secret operations such as stealing password or banking PIN (Personal Identification Number) or other personal information about user.
iii. It infects computers through installation of software form Internet.
iv. It slows down the performance of infected computer.
v. Most of the spyware is designed to be difficult to remove.

Examples of spyware:

For example, Flame is a spyware that was discovered in 2012. It attacks computers that use Microsoft Windows operating system. It is known as one of the most sophisticated spyware used for the purpose of espionage. It can record screenshots, keyboard activities and network traffic. It also has the capability to turn on the computer microphone and record conversation over Skype.

Detection of spyware by antivirus software is shown in Fig.

Spyware Alert!

Security Warning!

Worm.Win32.NetSky detected on your machine.
This virus is distributed via the Internet through e-mail and Active-x objects.
The worm has its own SMTP engine which means it gathers e-mails from your local computer and re-distributes itself.
In worst cases this worm can allow attachers to access your computer, stealing passwords and personal data.
Viruses can damage your confidential data and work on your computer.
Continue working in unprotected mode is very dangerous.

Type: Virus
System Affected: Windows 2000, NT, ME, XP, Vista, 7
Security Risk (0-5): 5
Recomendations: It is necessary to perform a full system scan.

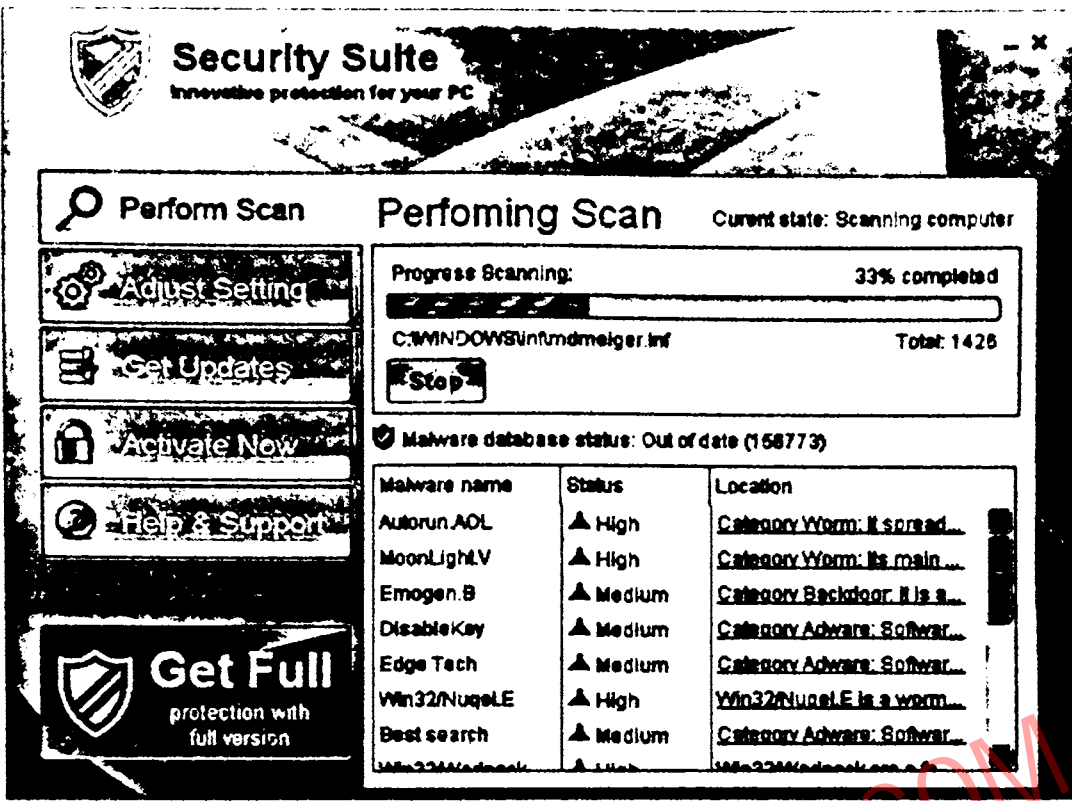
OK

Detection of spyware by antivirus software

Adware:

Adware is a malware that attaches itself to free software on the Internet and infects computer when such software is downloaded.

i. It pops up advertisements during execution of infected program.
ii. Pop-up block option in browsers helps protect computer from adware.
iii. Some adware may also collect user information without their permission.

Detection of adware and other malware are shown in Fig.

Detection of Adware and other malware by antivirus software

ii. Explain how malware spreads.

Ans: Spreading of Malware:

The following are different ways malware can spread in computers.

Infected Flash Drives/CDs:

Virus, spyware and other types of malware can infect computers in which anti-malware software is not installed through infected flash drives and CDs.

Pirated Software:

Software piracy refers to making of unauthorized copies of copyrighted software and distributing it. Pirated software on CDs is a very common source of spreading malware on computers because these are often infected.

If users download pirated music, movies, programs, etc. for free, their computers may be infected because pirated downloads often contain viruses, spyware or other malicious programs.

Network and Internet:

Computers connected to network get infected with malware when information is exchanged with other computers. Computers are also infected while using Internet when users download something or browse infected Web sites.

Computer may get infected with a virus or other malware if the user downloads software such as games, updates, demos and other programs from unreliable sources and installs it on the computer.

E-mail Attachments:

Opening e-mail attachments from a stranger or from an unknown address can infect computer with malware. Even downloading and opening e-mail from a friend or family member can be dangerous. They may pass the user a virus or other malware without knowing about it.

iii. Explain how to protect computer systems from virus attacks.

Ans: Protecting Computer from Malware/Virus Attacks:

We have to install the following software to safeguard computer against viruses, worms, adware and spyware.

- Antivirus software
- Anti-spyware software

Antivirus Software:

Antivirus software is a computer program that detects and removes viruses and other types of malware.

- Computer user should install it on computer and update it regularly.
- Most antivirus programs have an auto-update feature. This feature automatically updates the antivirus program through Internet so that it can detect and remove new versions of viruses as well.
- Whenever a user connects a flash drive or any other type of storage device to computer, he must run it through antivirus software to ensure that it does not contain virus.

Antivirus Programs:

Some commonly used antivirus programs are Norton Antivirus, Kaspersky Antivirus, AVG Antivirus, Bit Defender and McAfee Antivirus.

Anti-Spyware:

Anti-spyware is a computer program that detects spyware infections on computer and removes them. It helps to protect computer against security threats caused by spyware and other types of malware.

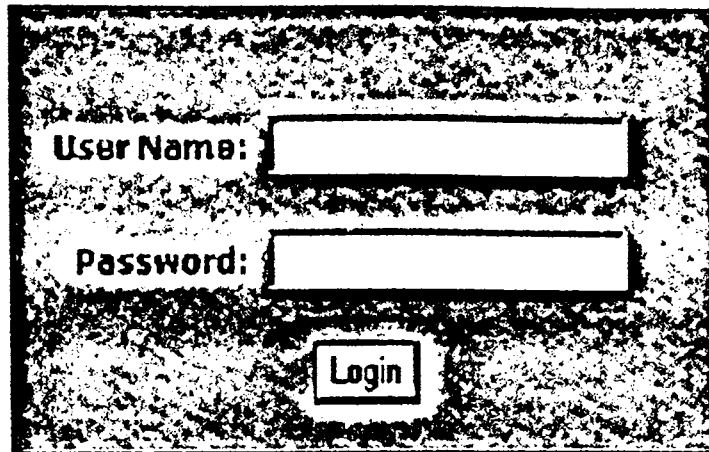
- Computer user should install it in computer and regularly update it to safeguard computer against new threats.
- Anti-spyware program runs in the background of computer and continually scans for spyware threats.
- A user can also start Anti-spyware program to scan computer to find and remove spyware.

Anti-spyware programs:

Some commonly used Anti-spyware programs are Norton Anti-spyware, SpySweeper, Spybot-Search & Destroy, Spyware Doctor, and AVG Anti-spyware.

iv. What are the common methodologies used for authentication?

Ans: Authenticaton Methodologies:

The following are common methodologies used for authentication purpose.

- Username and password
- Personal Identification Number
- Access card
- Biometrics

Username and Password:

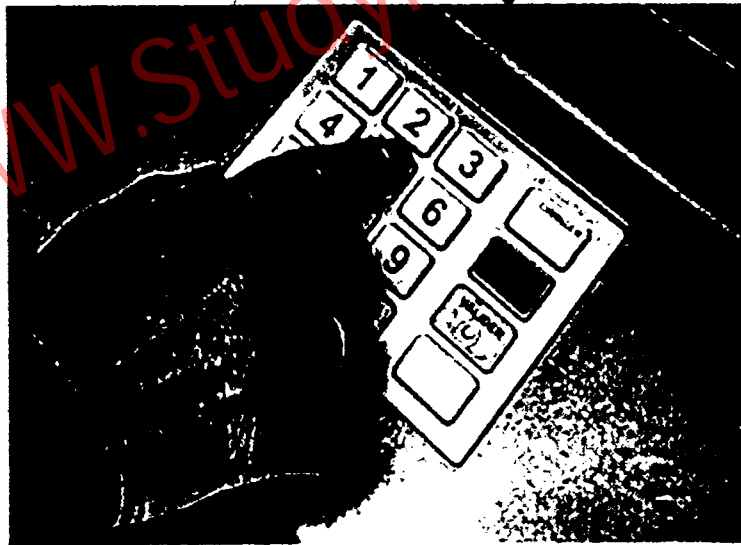
A username is a name that identifies a person on a computer system. Username is generally used with a password. The username and password combination is known as login information.

Username and password are used to authorize users to have access to computer systems, e-mail account, bank account and other services available on computer. Username is the known part of user's login information whereas password is secret. If it is known by a person it could be misused with bad intention. Window for entering login information is shown in Fig.

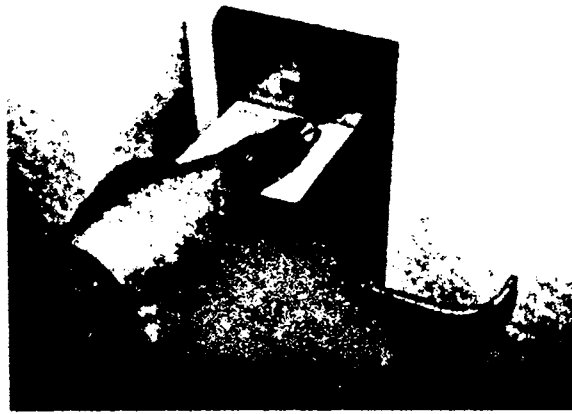
Window for entering username and password

Personal Identification Number (PIN):

PIN is a confidential numeric password used to authenticate a user to get access to a computer system. When a user enters the PIN, it is searched in the database stored in the computer. If it matches, the user is authorized to use the computer.

PINS are most commonly used with debit and credit cards in retail stores and many other places for payment of bills. It is also used with ATM cards to withdraw cash from ATM machines as shown in Fig.

Entering PIN on ATM machine

Access Cards:

Access cards are very similar in appearance to credit cards. They do not require username, password or PIN. They are commonly used to open security gates in offices and many other places as shown in Fig, where unauthorized people are not allowed to enter. Access cards are also used to open barriers in parking areas. They are an alternative to key for opening hotel room, etc.

Using access card for opening door of hotel room

Biometrics:

Biometrics refers to authentication methods based on physical characteristics of individuals such as features of face, hand geometry, retina, voice and fingerprint as shown in Fig.

Fingerprint biometrics machine used for time and attendance

It provides highly secure identification and personal verification technologies. Biometrics based systems are used for financial transactions, electronic banking and personal data privacy.

It provides more accurate authentication than using username and password or PIN. Biometrics is associated with a particular individual. Hence, it cannot be borrowed, stolen or forgotten. Forging in biometrics is practically impossible.

v. Define computer ethics and write some important moral guidelines for ethical use of computer technology.

Ans: Computer Ethics:

Computer ethics means an acceptable behavior for using computer technology. It is a code of behavior for moral and social issues while using computer technology, particularly Internet. Computer user should be honest, respect the rights of others on the Internet and obey laws that apply to online behavior.

We should not use bad language while chatting and social networking. We need to respect others views and should not criticize people.

We should not pretend as someone else and fool others. We should not download copyrighted material such as music, movies, etc. People should not do something on the Internet that is morally objectionable or illegal.

Ethical Use of Computer:

The following are some important moral guidelines for ethical use of computer technology.

i. Computer should not be used to harm other people.

ii. Computer users should not break into others' computer systems to steal, change or destroy information.

iii. Computer users should not read documents and e-mails of other users without their consent.

iv. People should not make illegal copies of copyright software and sell it for financial benefit.

v. Computer users who have special computer knowledge and ability should not create malicious software (such as computer virus) and spread it to other computers.

vi. People should not commit any type of crime with the help of computer technology.

vii. Computer users should respect the privacy of others.

Lab Activities

Activity:

Students should perform virus scan for hard disk drive of computer, USB flash drive, compact disk, etc. and remove any malware if detected by antivirus software.